JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 29, 1097-1107 (2013)

DOI:10.1688/JISE.2013.29.6.2

Impact of Identifier-Locator Split Mechanism on DDoS Attacks*

YING LIU, JIANQIANG TANG, MENG ZHANG AND HONGKE ZHANG
School of Electronic and Information Engineering
Beijing Jiaotong University
Beijing, 100044 P.R. China
E-mail: yliu@bjtu.edu.cn

The semantic overload of IP address, representing not only the identifiers of nodes but also the locators of nodes, is one of the fundamental reasons for hindering the development of current Internet. Therefore, the identifier-locator split mapping network which separates the two functions has become one of the federating themes for future Internet architecture. However, DDoS attacks are still in existence in this network. In this paper, we use the attack traffic to discuss and compare the effects of DDoS attacks on the current Internet and the identifier-locator split mapping network. The numerical and simulation analyses show that the identifier-locator split mapping network alleviates DDoS attacks more effectively compared with the current Internet.

Keywords: network security, identifier-locator split, DDoS attacks, LISP

1. INTRODUCTION

In recent years, the problems caused by routing scalability, security, and mobility in the current Internet have become notable and prominent [1-5]. The research shows that the main reasons for the above mentioned problems include the design principles of openness, trust, and autonomy embedded in the current Internet and the IP semantic overload problem [6, 7]. For example, in the aspect of security, since a traditional IP address contains a terminal's identity and location information, the correspondent node and the malicious eavesdroppers can obtain the terminal's identity information and topology location information from the IP address, resulting in the exposure of users' privacy. In addition, the attackers can easily use the dual attributes of an IP address to probe into the network topology, forge the identity information, and launch ARP spoofing, IP address spoofing, man-in-the-middle attacks, and distributed denial of service (DDoS) attacks, and so on.

Therefore, in the research of the next generation Internet structure, the design concept of splitting the identifier information from the locator information gets widespread concern and recognition. The main achievements are as follows: the network-based separation mechanism includes LISP (Locator/ID Separation Protocol) [8], IP^2 (IP-Based IMT Network Platform) [9, 10], Ivip (Internet Vastly Improved Plumbing) [11], TIDR (Tunneled Inter-domain Routing) [12] and the identifier-based universal network [13, 14]. The host-based separation mechanism, includes HIP (Host Identity Protocol) [15], Hi3 (Host Identity Indirection Infrastructure) [16], SHIM6 [17], LNP (Identifier Locator Net-

Received January22, 2013; accepted March 22, 2013.
Communicated by Ruay-Shiung Chang and Sheng-Lung Peng
* This work was partially supported by the National Natural Science Foundation of China under grant No. 612-02428, supported by the Fundamental Research Funds for Central Universities under grant No.2013JBM013.

work Protocol) [18, 19], and so on. Although these proposals are different, they are the solutions that all based on the separation of node identity information and location information aim to meet the needs of the future network. Compared with the host-based separation mechanism, the network-based separation mechanism has better routing scalability and users' location privacy, *etc*.

In this paper, we firstly make an in-depth study on the characteristics of the identifier-locator split mapping network (hereinafter referred to as split mapping network) and then compare the threats caused by DDoS attacks in the current network and the split mapping network respectively. Our results suggest that the split mapping network can effectively mitigate DDoS attacks. This paper is organized as follows: section 2 describes the model of split mapping network; section 3 presents a detailed theoretical analysis of the DDoS attacks in the current Internet and the split mapping network; section 4 demonstrates the calculation analysis and subsequently analyze the simulation results; the final section concludes with a summary of contributions and their implications.

2. THE IDENTIFIER-LOCATOR SPLIT MAPPING NETWORK MODEL

After studying and analyzing the architectures of the split mapping network which are proposed in the literature from [8] to [14], their common features are summarized as follows:

1. According to the topology position, the network is divided into two parts: the access network and the core network. The access network is a collection of various types of terminals or subnets, such as fixed, mobile, sensor networks, allowing access to the Internet. The core network is responsible for location managements and global routing. It is the essential requirement of the split mapping network to divide the network based on its topology information. Therefore, no matter when and where, an identity can never perform the dual functions of "identifier" and "locator".
2. For the data forwarding plane, separate of IP addresses into two numbering spaces: the Endpoint Identifier (ID) and the Routing Locator (LOC). The ID used in the access network represents the identity of a terminal. The IDs are assigned independently from the network topology. The essential sense of IDs requests that the identifier space should be plane structure, and there is no inevitable relationship between continuous identifier blocks. The LOCs used in the core network are responsible for global routing. The LOCs are aggregatable to guarantee the routing scalability and therefore the LOCs should be assigned topologically to network attachment points. Additionally, the IDs and the LOCs can't directly communicate with each other. They should be mapped to each other when the packets traverse the different space.
3. The mapping services between the ID and the LOC are realized by some specific devices. Usually, the router in the joint between the access network and the core network, known as Access Router (AR), is responsible for realizing the services. The mapping information of the whole network is stored in a specific device in the core network, distributedly or centralizedly. In this paper, except the access routers, all the devices in the core network maintaining the mapping information are referred to Mapping Servers (MS). Typically, the mapping information is updated by the "pull", "push" or the

hybrid manner. The "pull" means querying the external mapping information database for the mapping information and caching it to the local. The "push" refers to the way in which a mapping information database is copied to the AR to reduce the query latency. However, there exits scalability issues because of the restriction of the size of the mapping information database. The hybrid approach combines the two ideas to attain a balance between the two methods.

Therefore, without loss of generality and without considering the specific realization mechanism, the identifier-locator split mapping network model is shown in Fig. 1. In this model, AR is responsible for the access of terminals and the mapping services between IDs and LOCs. MS is responsible for storing and maintaining the mapping relationships between IDs and LOCs, providing the mapping registration and the query service for the access router. The Core Router (CR) forwards the packets according to the Locator.

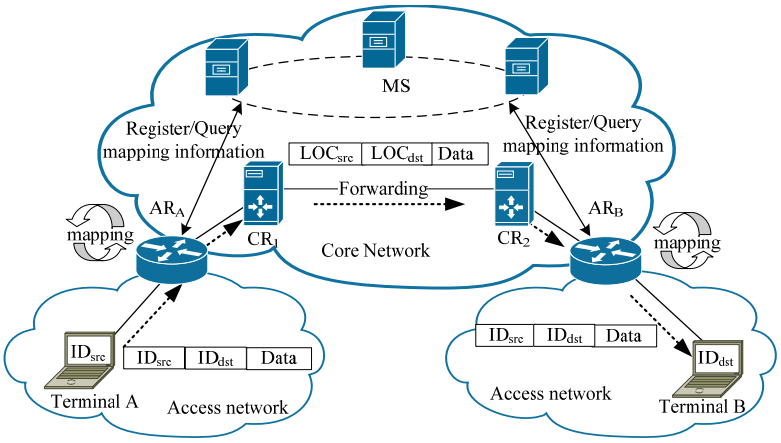

Fig. 1. The identifier-locator split mapping network model.

3. DDOS ATTACKS ANALYSIS

This paper uses the network topology in Fig. 2 to analyze the DDoS attacks in the current network and the split mapping network. In Fig. 2, the access routers are not distinguished between the current network and the split mapping network, represented uniformly with AR.

As shown in Fig. 2, the network is a fully connected network, in which any two hosts have access to each other. In this network, host A is a hostile attack host. The hosts represented by D_1, D_2, …, D_n and T_1, T_2, …, T_m are all common hosts. The hosts T_1, T_2, …, T_m are connected to the same sub-network through AR_2. In this topology, it is assumed that the attack target of host A is host T_2, so the access network to which AR_2 is connected is defined as the local link in this paper and the number of hosts is m. Other access networks are non-local links and the number of hosts is n.

The reference [20] generally classifies DDoS attacks into two types, the utilization of software vulnerability and the flow attack, and this paper will analyze the DDoS flow

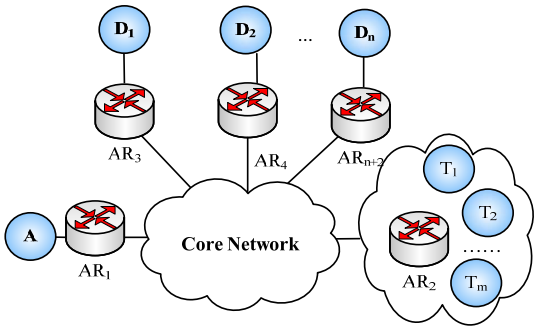

Fig. 2. Network topology.

attack. According to the analytical procedure in [21], this paper uses the attack traffic received by the victim to measure DDoS attacks effect. To generate the maximum amount of the attack traffic, host A will control as many hosts as possible to launch the DDos attacks to host T_2. Therefore, in this network, except the attack host A and the target host T_2, other hosts are likely to be controlled by the attack host A as bots. In addition, to better quantitatively analyze the DDoS attacks in the two types of networks, this paper proposes the following hypotheses.

For DDoS attacks, the attack traffic generated by the bots which are located in the non-local links is smaller than that generated by the bots located in the local link [22]. In the Fig. 2, to make it simple, suppose that the maximum attack traffic generated by the bots in the non-local links is b (Mbps) and the maximum attack traffic generated by the bots in the local link is c times as much as b (Mbps), and then the maximum attack traffic generated by the bots in the local link is cb (Mbps). Besides, it is assumed that the attack traffic generated by the attacker is not more than the maximum bandwidth of the local link. The attacker's ability is limited, so it can only control some of the hosts in the network. Suppose that the number of bots is k, and for the attack host A, it is of the same difficulty to control any of the hosts in the network.

In the current network, the attacker can obtain a terminal's identity information and location information from the terminal's IP address. To generate more attack traffic, the attacker will first choose the hosts in the local link as bots. However, since the location privacy is protected in the split mapping network, the attacker can only obtain the terminal's identity information rather than the location information; therefore, the attacker can only control the randomly selected hosts and then launch attack. This feature can effectively mitigate the threat caused by the DDoS attacks. The following part will make a detailed analysis of the DDoS attacks in the current network and the split mapping network.

3.1 Analysis of the Current Network

In the current network, the attacker can obtain a terminal's identity information and location information from the terminal's IP address, so the attacker will choose as many hosts in the local link as possible. Based on this hypothesis, in the current network, suppose the maximum DDoS attack traffic generated by host A is F_t, then:

$$F_t = \begin{cases} k * c * b & k < m-1 \\ (k-m+1) * b + (m-1) * c * b & k \geq m-1 \end{cases} \tag{1}$$

3.2 Analysis of the Identifier-Locator Split Mapping Network

In the split mapping network, since the attacker is unable to obtain a terminal's location information, the attacker can only control the randomly selected hosts instead of finding the hosts correctly which can do the maximum damage to the target host. Therefore, according to this hypothesis, when $k < m - 1$ the maximum attack traffic that the DDoS attacker can generate has $k + 1$ possible situations, which are shown as follows.

Possible situation 1: All the randomly selected hosts are in the non-local links of target host T_2, and now the maximum attack traffic is $F_{s0} = k * b$.

The probability of this situation is $P_{s0} = \dfrac{C_n^k}{C_{n+m-1}^k}$.

Possible situation 2: Only one of the randomly selected hosts is in the local link of target host T_2, and now the maximum attack traffic is $F_{s1} = (k - 1) * b + c * b$.

The probability of this situation is $P_{s1} = \left\{ \dfrac{C_n^{k-1} C_{m-1}^1}{C_{n+m-1}^k} \right.$.

Possible situation $k + 1$. k of the randomly selected hosts are in the local link of target host T_2, and now the maximum attack traffic is $F_{sk} = k * c * b$.

The probability of this situation is $P_{sk} = \dfrac{C_n^0 C_{m-1}^k}{C_{n+m-1}^k}$.

At this moment, the average maximum attack traffic that the DDoS attacker can generate is:

$$F_{sa} = \sum_{i=0}^{k} \frac{C_n^{k-i} C_{m-1}^i}{C_{n+m-1}^k} \left[(k-i) * b + i * c * b \right]. \tag{2}$$

Similarly, when $k \geq m - 1$, the situation is:

$$F_{sb} = \sum_{i=0}^{m-1} \frac{C_n^{k-i} C_{m-1}^i}{C_{n+m-1}^k} \left[(k-i) * b + i * c * b \right]. \tag{3}$$

To sum up, in the split mapping network, the average maximum attack traffic that the DDoS attacker can generate is:

$$F_s = \sum_{i=0}^{\min\{k, m-1\}} \frac{C_n^{k-i} C_{m-1}^i}{C_{n+m-1}^k} \left[(k-i) b + i * c * b \right]. \tag{4}$$

4. THE NUMERICAL ANALYSIS

This part presents the concrete numerical analysis and the calculation of Eqs. (1) and (4). We suppose that the number of hosts in the non-local links is n = 100, the attack traffic generated by each bot in the non-local links is b = 1(Mbps), and the attack traffic generated by each bot in the local link is c times as much as that generated by each bot in the non-local links, with c = 5. F_t, the attack traffic generated by the current network, is shown in Fig. 3 and F_s, the attack traffic generated by the split mapping network, is shown in Fig. 4 where m, representing the number of hosts in the local link, varies from 2 to 50 and k, representing the number of attack hosts, varies from 1 to 100. In the two figures, the different colors in the fill area represent different amounts of attack traffic and the specific numerical values are corresponding to the color bar at the right hand of the Figures. From Figs. 3 and 4, it can be found that in the same network topology environment, as m and k increase, the attack traffic in the two networks increase as well. But, under the same condition, the attack traffic in the split mapping network is less than that in the current network.

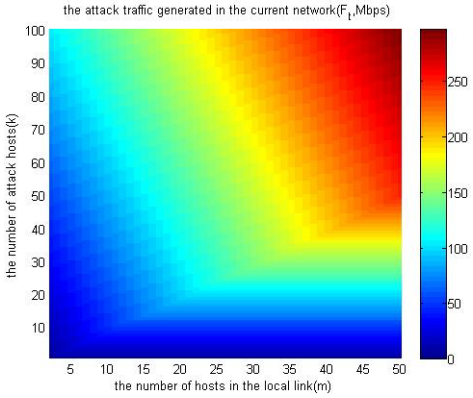

Fig. 3. Variation of the attack traffic generated in the current network results from the changes in the values of m and k.

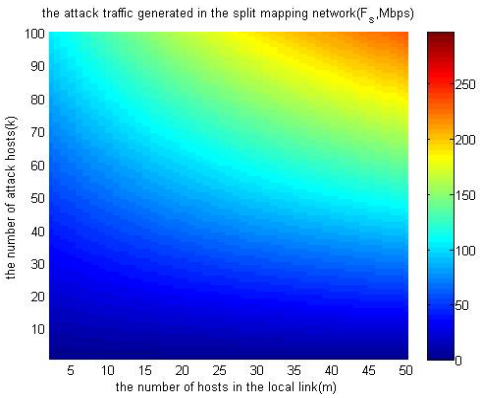

Fig. 4. Variation of the attack traffic generated in the split mapping network results from the changes in the values of m and k.

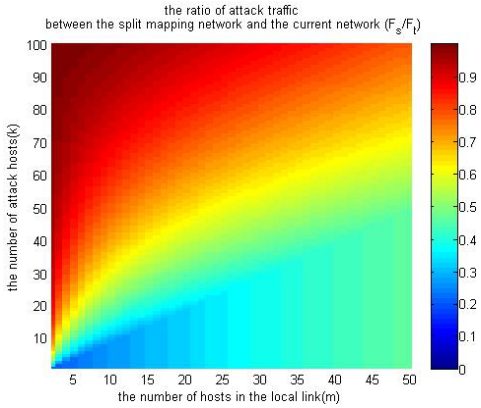

Fig. 5. the ratio of attack traffic between the split mapping network and the current network.

Fig. 5 shows the ratio of attack traffic between the split mapping network and the current network when the numerical value of m and k are as mentioned above. The calculation result shows that compared with the attack traffic in the current network, the attack traffic in the split mapping network can be reduced by 79% at most and 37% in average. Only when m is small, and k is much larger than m, can the attack traffic in the split mapping network be closed to that in the current network. It can be found from Figs. 3 and 4 that under this condition, the attack traffic in both networks remain relatively small. Thus, it can be seen that the split mapping network can better mitigate the bad influences caused by the DDoS attacks.

The following part analyzes the attack traffic in both networks where the numerical value of m is fixed and the numerical value of n and k is changing. F_t and F_s are shown in Figs. 6 and 7 respectively where m is 20, b is 1, c is 5, n is from 60 to 150 and k is from 1 to 40.

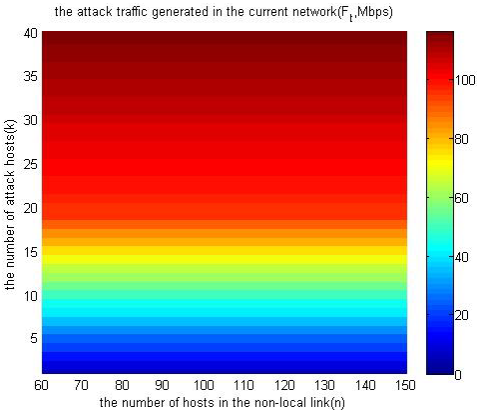

Fig. 6. Variation of the attack traffic generated in the current network results from the changes in the values of n and k.

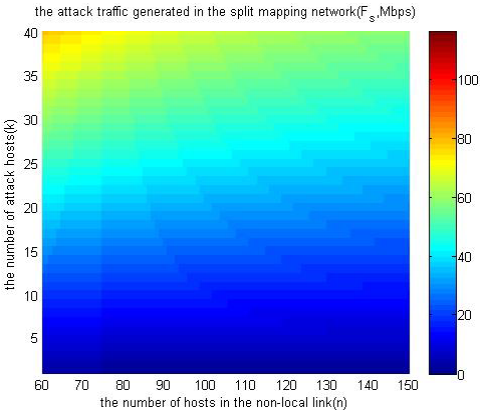

Fig. 7. Variation of the attack traffic generated in the split mapping network results from the changes in the values of n and k.

From Fig. 6, it can be found that in the current network, when the number of hosts in the local link is fixed (m = 20), the attack traffic increases with the increase of the number of bots and when the number of hosts in the non-local link is big enough, the attack traffic is not influenced by the change of the number of hosts in the non-local links. From Fig. 7, it can be seen that in the split mapping network, as k increases, the attack traffic increases as well, but obviously it is less than the attack traffic generated in the current network under the same condition. In addition, with the further increase of n, the attack traffic will become smaller and smaller, gradually approaching to the situation where all the bots are the hosts in the non-local links. Fig. 8 shows the ratio of attack traffic between the split mapping network and the current network when the numerical value of n and k are as mentioned above. The calculation result shows that compared with the attack traffic in the current network, the attack traffic in the split mapping network can be reduced by 71% at most, 43% at least, and 60% in average. Thus, it can be seen that the split mapping network can better mitigate the bad influences caused by the DDoS attacks.

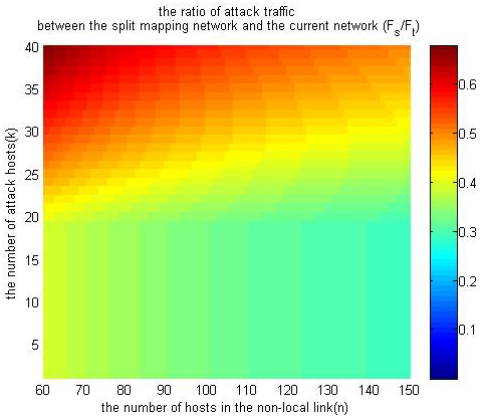

Fig. 8. The ratio of attack traffic between the split mapping network and the current network.

5. THE SIMULATION ANALYSIS

This part makes the simulation for the network topology shown in Fig. 2 by OMNet++ [23]. We mainly simulate the attack traffic received by the target host in 10 seconds in the following two situations.

Situation 1: supposing *n*, the number of hosts in the non-local link, is 200, and *m*, the number of hosts in the local link, is 20, and *k*, the number of attack hosts, is respectively 5, 20, and 35, the simulation of the attack traffic received by the target host in the current network and in the split mapping network is shown in Fig. 9.

From Fig. 9, it can be seen that when the number of hosts in the non-local links and in the local link is fixed, with the increase of the number of bots, the attack traffic received by the target host in the current network and in the split mapping network will increase as well. But, as shown in Fig. 9, when *k* is 5, 20, and 35 respectively, compared with the average DDoS attack traffic generated in the current network, the average DDoS

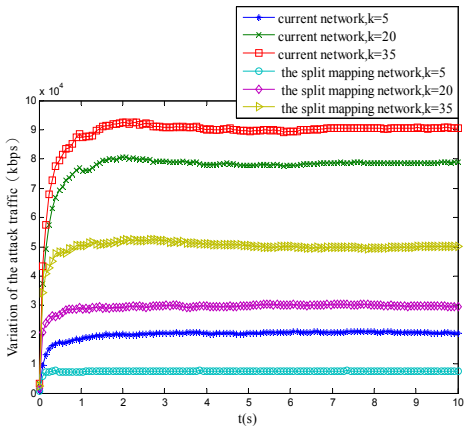

Fig. 9. Variation of the attack traffic results from the different values of *k,* when *n* and *m* are fixed to 200 and 20 respectively.

attack traffic generated in the split mapping network is reduced by 63%, 62%, and 44% respectively, which suggests that the split mapping network reduces the influences of DDoS attacks. At the same time, it can be also found that the smaller the number of bots is, the more obvious the mitigation effect is. In the actual network environment, the number of bots is much smaller than the total number of hosts in the network, so in the actual environment, the split mapping network can better mitigate the DDoS attacks.

Situation 2: supposing that n, the number of hosts in the non-local link, is 200, and k, the number of attack hosts, is 20, and m, the number of hosts in the local link, is respectively 10, 20, and 30, the simulation of the attack traffic received by the target host in the current network and in the split mapping network is shown in Fig. 10.

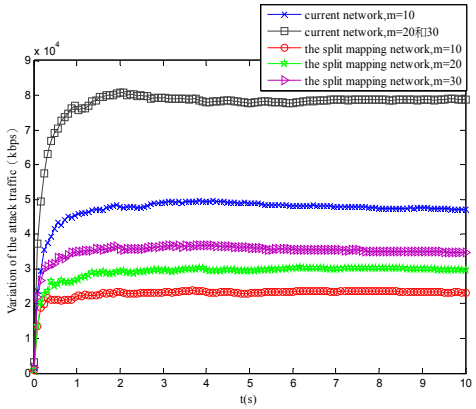

Fig. 10. Variation of the attack traffic results from the different values of m, when n and k are fixed to 200 and 20, respectively.

In Fig. 10, when m is respectively 10, 20, and 30, compared with the average DDoS attack traffic generated in the current network, the average DDoS attack traffic generated in the split mapping network is reduced by 51%, 62%, and 54% respectively. When $m = k = 20$, the attack traffic generated in the current network will reach the maximum (when all the bots are the hosts in the local link); later, with the increase of m, the attack traffic generated in the current network no longer increases, but the attack traffic generated in the split mapping network keeps increasing all the time, so the percentage of the reduced attack traffic will decrease. In general, in the actual network environment, the number of hosts in the local link is smaller than the number of hosts in the non-local links, so the split mapping network's role in mitigating the DDoS attacks is still obvious.

The simulation results of the two situations mentioned above show that in the actual network environment, the split mapping network can better mitigate the influences caused by the DDoS attacks, which is consistent with the results of the theoretical analysis and numerical analysis.

6. CONCLUSION

As a new type of network architecture, the identifier-locator split mapping network has several advantages compared with the current network. It successfully separates a

user's identity information from the location information, and protects the user's location privacy. This paper analyzes the split mapping network's role in mitigating DDoS attacks and gives out the quantitative analysis results. The numerical and simulation analysis indicate that the identifier-locator split mapping network is more effective in mitigating DDoS attacks compared with the current network.

REFERENCES

1. BGP Report, http://bgp.potaroo.net/.
2. http://www.cert.org.cn/articles/docs/common/2011042225342.shtml.
3. N. Nakajima, A. Dutta, S. Das, *et al.*, "Handoff delay analysis and measurement for SIP based mobility in IPv6," in *Proceedings of IEEE International Conference on Communications*, Vol. 2, 2003, pp. 1085-1089.
4. R. Koodli, "IP address location privacy and mobile IPv6: Problem statement," RFC 4882, 2007.
5. Q. Feng, L. Xiaoqian, S. Wei, *et al*., "A novel location management scheme based on DNS in proxy mobile IPv6," *Journal of China Communications*, Vol. 7, 2010, pp. 43-52.
6. J. Saltzer, "On the naming and binding of network destinations." RFC 1498, 1993.
7. D. Clark, R. Braden, A. Falk, *et al.*, "FARA: Reorganizing the addressing architecture," in *Proceedings of ACM SIGCOMM Workshop on Future Directions in Network Architecture*, 2003, pp. 313-321.
8. D. Farinacci, V. Fuller, D. Meyer, *et al*., "Locator/ID separation protocol (LISP)," Internet Draft, draft-farinacci-lisp-15.txt, 2011.
9. H. Yumiba, K. Imai, and M. Yabusaki, "IP-based IMT network platform," *Journal of IEEE Personal Communications Magazine*, Vol. 8, 2001, pp. 18-23.
10. T. Okagawa, K. Nishida, and A. Miura, "A proposed routing procedure in IP^2," in *Proceedings of Vehicular Technology Conference*, Vol. 3, 2003, pp. 2083-2087.
11. R. Whittle, "Ivip (Internet Vastly Improved Plumbing) architecture," Internet Draft, draft-whittle-ivip-arch-04, 2010.
12. J. J. Adan, "Tunneled inter-domain routing (TIDR)," Internet Draft, draft-adan-idr-tidr-01, 2006.
13. Z. Hongke and S. Wei, "Fundamental research on the architecture of new network – Universal network and pervasive services," *Journal of Acta Electronica Sinica*, Vol. 35, 2007, pp. 593-598.
14. D. Ping, Q. Yajuan, and Z. Hongke, "Research on universal network supporting pervasive services," *Acta Electronica Sinica*, Vol. 35, 2007, pp. 599-606.
15. R. Moskowitz, "Host Identity Protocol architecture (HIP)," Internet Draft, draft-ietf-hip-rfc4423-bis-03, 2011.
16. P. Nikander, J. Arkko, and B. Ohlman, "Host identity indirection infrastructure," in *Proceedings of the 2nd Swedish National Computer Networking Workshop*, 2004, pp. 1-4.
17. E. Nordmark and M. Bagnulo, "Shim6: Level 3 multihoming shim protocol for IPv6," RFC 5533, 2009.
18. R. Atkinson and S. Bhatti, "An introduction to the identifier-locator network proto-

col (ILNP)," in *Proceedings of London Communications Symposium*, 2006.
19. R. J. Atkinson, "ILNP concept of operations," Internet Draft, draft-rja-ilnp-intro-11, 2011.
20. A. Hussain, J. Heidemann, and C. Papadppoulos, "A framework for classifying denial of service attack," in *Proceedings of the ACM SIGCOMM Workshop on Applications, Technologies, Architectures, and Protocols for Computer Communications*, 2003, pp. 99-110.
21. K. Jiejun, M. Mirza, J. Shu, *et al*., "Random flow network modeling and simulations for DDoS attack mitigation," in *Proceedings of IEEE International Conference on Communications*, Vol. 1, 2003, pp. 487-491.
22. W. Chunfeng, J. G. Hurwitz, H. Newman, *et al*., "Optimizing 10-gigabit ethernet for networks of workstations, clusters, and grids: A case study," in *Proceedings of ACM /IEEE Conference on Supercomputing*, 2003, pp. 50-62.
23. OMNET++3.3, http://www.omnetpp.org.